

SHCreateDirectory

Vulnerable to TOCTOU issues

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 7003 bytes

Attack Category	<ul style="list-style-type: none">• Path spoofing or confusion problem	
Vulnerability Category	<ul style="list-style-type: none">• Indeterminate File/Path• TOCTOU - Time of Check, Time of Use	
Software Context	<ul style="list-style-type: none">• File Management	
Location	<ul style="list-style-type: none">• shlobj.h	
Description	SHCreateDirectory creates a directory/folder. SHCreateDirectory is vulnerable to TOCTOU attacks.	
APIs	Function Name	Comments
	SHCreateDirectory	use
	SHCreateDirectoryEx	use
Method of Attack	<p>The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results.</p> <p>The mknod() call is a use-category call, which when preceded by a check-category call can be indicative of a TOCTOU vulnerability.</p> <p>A TOCTOU attack in regards to SHcreatedirectory() can occur, for example, when</p> <ol style="list-style-type: none">a. A check for the existence of a directory (check call) occursb. SHcreatedirectory() is executed <p>Between a and b, an attacker could, for example, create a link from the targeted directory to a different known directory. The subsequent access of the target</p>	

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

	directory would result in minimally, potentially erroneous program function.		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Generally applicable.	Utilize a file descriptor version of stat/ fstat when checking.	Effective
	Generally applicable.	The most basic advice for TOCTOU vulnerabilities is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help to limit the false sense of security given by the check.	Does not resolve the underlying vulnerability but limits the false sense of security given by the check.
	Generally applicable.	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Recheck the resource after	Effective in some cases.

		the use call to verify that the action was taken appropriately.	
Signature Details	int SHCreateDirectory(HWND hwnd,LPCWSTR pszPath);		
Examples of Incorrect Code	<pre>int use_status; struct stat statbuf; check_status=stat("C:\\\\xxxx\\pub \\download\\windows\\dotnet", &statbuf); [...] int res = SHCreateDirectory(NULL, L"C:\\\\xxxx\\pub\\download\\win- dows\\dotnet"); [...]</pre>		
Examples of Corrected Code	<pre>[...] int res = SHCreateDirectory(NULL, L"C:\\\\xxxx\\pub\\download\\win- dows\\dotnet"); [...]</pre>		
Source References	<ul style="list-style-type: none"> • Viega, John & McGraw, Gary. <i>Building Secure Software: How to Avoid Security Problems the Right Way</i>. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152, ch. 9 • http://www.awprofessional.com/articles/article.asp?p=23947&seqNum=3&rl=1² • http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shcreatedirectory.asp³ 		
Recommended Resources	<ul style="list-style-type: none"> • MSDN reference for SHCreateDirectory⁴ • MSDN reference for SHCreateDirectoryEx⁵ 		
Discriminant Set	Operating System	<ul style="list-style-type: none"> • Windows 	
	Languages	<ul style="list-style-type: none"> • C • C++ 	

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>